벤처창업연구 제17권 제4호 (통권82호)
Asia-Pacific Journal of Business Venturing and Entrepreneurship Vol.17 No.4 pp.163-172

ISSN 1975-7557
e-ISSN 2671-9509

디지털 헬스케어 서비스 제공자의 정보보호의도에 관한 연구

양창규 (아주대학교 경영대학 e-비즈니스학과 겸임조교수)*

국 문 요 약

본 연구는 디지털 헬스케어 서비스 제공자의 보호동기를 형성하는 위험평가와 대처평가가 정보보호의도의 주요한 요인인 유도통제의도와 자기방어의도에 미치는 영향을 확인하고자 한다. 연구모형은 보호동기이론을 기반으로 기존 선행연구를 통해 심각성, 취약성, 반응효능감, 자기효능감을 독립변수로 채택하였다. 연구모형 검증을 위해 한국의 디지털 헬스케어 서비스 기업 임직원 222명을 대상으로 설문조사를 실시하였으며, 데이터는 구조방정식을 사용하여 분석하였다. 연구결과에 따르면 (1) 보안위협의 결과에 대한 명확한 인지가 디지털 헬스케어 서비스 제공자의 정보유출 사고에 대한 심각성에 대한 이해를 높여주고, 이를 통해 디지털 헬스케어 서비스 제공자의 오남용을 줄일 수 있으며, (2) 보안시스템에 대한 디지털 헬스케어 서비스 제공자의 신뢰와 만족이 스스로 정보유출에 대응할 수 있다는 자신감을 형성시킬 수 있고, (3) 디지털 헬스케어 서비스 제공자는 정보유출로 인해 돌아오는 결과를 인지하고 있지만, 실제 자신에게 발생할 수 있는 가능성은 적다고 생각하고 있음을 확인하였다. 이 연구결과는 디지털 헬스케어 서비스를 운영하는 벤처기업은 디지털 헬스케어 서비스 제공자의 정보보호의도를 높이기 위해서 디지털 헬스케어 서비스 제공자의 보안수준을 높일 수 있는 지속적인 콘텐츠 제공이 필요하고, 타 벤처기업대비 높은 수준의 보안시스템을 도입하여 디지털 헬스케어 서비스 제공자의 신뢰를 통해 정보보호 동기유발이 중요하다는 점을 시사한다.

핵심주제어: 정보보호의도, 디지털 헬스케어, 보호동기이론, 건강정보보호

Ⅰ. 서론

헬스케어 서비스 공급에 대한 비용절감의 기회와 다양한 헬스케어 서비스를 공급할 수 있다는 측면에서 헬스케어 서비스와 ICT의 융합을 통한 벤처기업의 창업이 가속화되고 있다(Agarwal et al., 2010; Peppard & Ward, 2016; 안정민, 2021). 이러한 패러다임은 그간의 전통적인 전자의무기록이나 의료영상정보시스템 분야부터 질병관리 소프트웨어나 생체신호를 계측과 더불어 다양한 종류의 데이터를 통합하고 분석하는데까지 이르렀다(김호다·주애란, 2021; 소현정·곽기영, 2021). 또한, 분산되어 있는 헬스케어 정보의 통합과 함께, 모바일 기기를 통해 언제, 어디서나 디지털화 하여 건강관리 등을 포함한 통합된 헬스케어 서비스를 제공하는 것이 가능해지고 있다(Hurson et al., 2004; Wu et al., 2011; 박아름 외, 2020; 양재민 외, 2020). 간단하게는 처방전이나 약봉투를 사진으로 찍어 앱에 등록하면 이용자의 복약일정, 진료기록이 손쉽게 관리되는 파프리카케어와 같은 모바일 앱부터 이용자의 유전체 정보를 제공받아 전반적인 건강상태를 관리해주는 휴먼스케이프나 치료, 시술, 약 처방 등 진료기록 전반을 관리해주는 이지케어텍과 같은 의료 빅데이터 기업까지 다양한 헬스케어 서비스가 존재한다. 최근에는 카카오나 네이버 등도 의료 빅데이터 기업과 협업하여 디지털 헬스케어 서비스 시장에 진출하기 시작했다. 이처럼 디지털 헬스케어 서비스 시장 확대에 따른 긍정적인 측면으로 인해 새로운 디지털 헬스케어 서비스를 제공하는 벤처기업의 출현과 투자 증가가 가속되고 있지만, 다양한 헬스케어 서비스의 통합과 여러 기업의 시장 진입으로 인해 이용자의 의료 또는 건강 정보의 유출 등 부정적인 측면에 대한 우려가 있는 것도 현실이다(Anderson & Agarwal, 2011; Choi et al., 2017; 권혁준 외, 2018). 그간 정보유출의 사례만 보더라도 의료정보 서비스에 ICT가 도입된 이후 지속적으로 이용자의 진료기록이 노출되어 왔고, 디지털 헬스케어 서비스가 보편화되고 있는 현재까지 다양한 보안사고 사례가 발생해 왔다. 특히, 디지털 헬스케어 서비스가 소프트웨어 및 네트워크 연결성이 강화되면서 네트워크 프로토콜 기반의 보안사고도 증가하고 있다. 또한, 모바일 기기를 통해 디지털 헬스케어 서비스에 대한 접근성이 좋아지면서, 디지털 헬스케어 서비스 제공자의 낮은 보안의식으로 인한 보안사고도 다수 발생하고 있다(박민정 외, 2018).

벤처기업의 ICT서비스가 성공적으로 시장에 정착하기 위해서는 ICT서비스의 이용자, 서비스 제공자 등의 적극적인 참여와 서비스 만족도나 정보보안 신뢰도 측면에서 주변 지인들로의 네트워크 효과가 매우 중요하다. 따라서, 디지털 헬스케어 서비스에서 다뤄지는 질병, 건강상태, 치료의 경과 등과 같은 민감한 정보들이 안전하게 취급될 필요가 있다. 또한,

* 주저자, 아주대학교 경영대학 e-비즈니스학과 겸임조교수, cozlove@ajou.ac.kr
· 투고일: 2022-04-26 · 1차 수정일: 2022-07-02 · 2차 수정일: 2022-08-05 · 게재확정일: 2022-08-17

디지털 헬스케어 서비스의 보안사고는 건강한 삶을 위해 이용하고 있는 이용자에게 2차적인 정신적 피해를 야기할 수 있고, 다양한 범위에 활용이 가능하며 사회적으로도 큰 피해가 발생할 수 있기 때문에 철저한 보안이 요구된다(Solove & Schwartz, 2014). 그러나, 그간 디지털 헬스케어 서비스의 보안에 대한 연구는 주로 기술적인 측면의 연구가 주류를 이루었다(Gritzalis & Lambrinoudakis, 2004). 실제 디지털 헬스케어 서비스 내 정보유출은 주로 디지털 헬스케어 서비스 제공자의 오남용과 관리소홀로 인해 발생할 여지가 큼에도 불구하고 보안정책과 보안시스템에만 관심을 가졌기 때문에, 실제로 보안정책을 준수하여야 하는 디지털 헬스케어 서비스 제공자의 의도에 의한 보안사고의 원인을 파악하는데 한계점이 있었다고 할 수 있다.

따라서, 본 연구는 디지털 헬스케어 서비스 제공자의 정보보호의도에 주된 관심을 가진다. 즉, 디지털 헬스케어 서비스의 보안사고 예방을 위해 어떠한 요인이 실제 디지털 헬스케어 서비스 제공자에게 어떠한 영향을 주고, 이들의 정보보호의도가 형성되는지 파악하고자 한다. 이를 위해, 보호동기이론을 이용한 연구모형을 고안하여 디지털 헬스케어 서비스 제공자의 정보보호의도에 영향을 미치는 요인을 파악하는데 그 목적이 있다. 특히, 정보보호의도에 미치는 주요한 요인에 따라 디지털 헬스케어 서비스의 보안정책, 보안시스템의 개선을 위한 전략이 크게 달라질 수 있기 때문에, 디지털 헬스케어 서비스를 제공하고 있는 벤처기업과 보안서비스 제공기업, 디지털 헬스케어 서비스 제공자 모두에게 큰 도움이 되리라 판단된다.

II. 이론적 배경

2.1. 디지털 헬스케어 서비스

유비쿼터스 환경에 진입하면서 의료정보분야에 다양하고 새로운 의료서비스의 필요성이 인식되었다. 이러한 관점에서 많은 의료기관들이 진료, 진료지원, 진단부터 비용 수납까지 모든 의료 서비스를 포괄하는 의료정보시스템을 도입하였다. 이는 의료기관의 진료와 관련된 다양한 의사결정, 의료서비스의 질 향상 및 효율적인 의료서비스 운영 등을 지원하기 위한 시스템으로 정의되었다(정준호·김정숙, 2015). 따라서, 이미 2000년부터 전자의무기록 도입 등의 의료정보의 디지털화가 본격적으로 이뤄지기 시작했고, 정부의 국민건강보험제도와 연계되는 등 보다 폭넓게 사용되어지게 되었다. 최근 들어, 이러한 디지털 의료정보 서비스는 ICT와 선진 의료서비스가 결합된 디지털 헬스케어 서비스라는 측면에서 응용환경에 따라 다양하게 확산되었는데, 주로 의료기관 중심의 홈 헬스케어 서비스와 BAN(Body Area Network) 중심의 개인 헬스케어 서비스로 나뉜다(윤은준, 2012; 엄혜미, 2021). 의료기관이 중심이 된 질병의 진단 또는 치료뿐만 아니라 이용자와 함께 예방과 건강관리가 더해진 개념의 디지털 헬스케어 서비스의 시장규모도 급격하게 성장하고 있다(이성경 외, 2020). 또한, 예방과 건강관리에 관련된 서비스의 성장도 크게 성장하고 있어, 4차 산업과 동반하여 많은 벤처기업들이 시장에 진입하고 있고 지속적으로 성장될 것으로 예상되고 있다(임성훈·김용태, 2015; 김영수·정재진, 2019).

2.2. 의료정보유출

광범위하게 디지털 헬스케어 서비스를 활용하고 있는 미국의 경우 의료정보보호에 가장 앞서 있는 실정이다. 이미 1996년 의료정보보호법(HIPAA)을 규정했고, 2009년에는 전자의무기록 체계를 만들어 진료와 연구 목적의 다양한 디지털 정보를 활용하기 위한 의료정보기술법(HITECH)까지 제정한 바 있다(Guadarrama, 2018). 그러나, 스마트폰이 보편화 되면서 스마트폰을 통한 의료정보 이용이 증가하고 의료정보보호 위반 제소가 증가했고, 과징금 부과액도 지속적으로 증가하고 있는 상황이다(Gonsalves, 2018). 반면에 한국은 현행법 상 의료정보에 대한 명확한 정의가 규정된 바는 없으나, 여러 연구자들이 환자의 진료과정에 얻어진 사적인 부분을 포함한 자료나 건강을 유지하는데 필요한 건강에 대한 정보로 의료정보를 정의하고 있다(김강한, 2016; 이한주, 2014). 이와 같이 의료정보는 다른 개인정보보다 민감한 정보를 포함하고 있고, 이를 조합하여 다양하게 활용할 수 있기 때문에 보안에 보다 엄격해야만 하지만 최근까지 정보유출 사례가 지속적으로 발생해 왔다(Kokolakis, 2017). 의료정보가 유출되는 사례와 범위는 매우 다양한데 미국의 경우 무단으로 빅데이터 기업에 의료정보를 제공하거나 제약업체의 리베이트를 위한 의료정보 유출과 같이 서비스 제공자가 원인인 경우뿐만 아니라 외부 해킹 등으로 인한 외부가 원인인 경우도 있다. 국내의 경우에도 유사한 사례들이 발생하고 있는데, 2020년 2월 의료법 개정 후에도 2년간 총 25개 병원에서 해킹 및 전자침해사고발생이 있었고, 종합병원급 이상에서도 8건이나 발생하였다(박광하, 2021). 주로 서비스 제공자의 PC나 스마트폰을 통해 해킹이나 렌섬웨어와 DDos공격의 형태로 의료정보에 대한 유출이 시도되었다(김영신, 2021). 따라서, 향후에도 디지털 헬스케어 서비스 제공자를 경유하는 의료정보 유출에 대한 위험이 더욱 더 증가될 것으로 예상된다. 특히, 최근 한 대학병원에서 의료정보 유출에도 불구하고 피해자 보호나 재발방지 대책마련보다는 해명위주의 대응으로 사회적 무리를 일으킨 경우도 있어 의료정보보호에 맞게 개인정보보호법을 세분화하자는 의견도 있다(함민정, 2022)

2.3. 보호동기이론

개인의 보호동기를 파악하는 매개변수를 찾아내려는 다양한 연구가 시도되고 있다(Ajzen, 1991; Lee et al., 2004; 장철호·차윤호, 2021). 그러나, 그간 연구에서 도입한 개념들은 개인의 보호동기를 포괄적으로 파악할 수 없는 단편적인 변수를 사용했다는 한계가 있다. 때문에, 본 연구에서는 Edwards(1954)의 보호동기이론을 매개변수로 활용하고자 한다. 보호동기이론은 기대-가치이론에 영향을 받아 Rogers(1983)가 확립한 이론으로 사회학분야에서 널리 사용되는 이론이다(Edwards, 1954; Rogers, 1983). 보호동기이론은 개인의 보호행동을 예측하는데 가장 훌륭한 이론 중 하나로, 보호동기를 위험평가와 대처평가로 구분한다(Anderson & Agarwal, 2011). 위험평가는 개인은 위험을 느끼면, 그 위험이 가져올 결과의 심각성과 자신이 위험에 노출될 취약성에 의해 이뤄진다. 이와 함께, 대처평가는 개인은 위험을 자신의 능력으로 해결할 수 있다는 자기효능감과 행동이 실제로 위험을 피할 수 있는가에 대한 반응효능감에 따라 이뤄진다(Rogers, 1983). 또한, 여러 연구자들이 정보보호의도 연구에 보호동기 이전의 원인을 파악하기 위한 노력도 시도되고 있다(Vance et al., 2012). 때문에, 정보보호의도에 미치는 영향의 매개변수로 보호동기이론을 활용하는 것은 개인의 정보보호의도 형성을 보다 구체적으로 파악할 수 있다고 할 수 있다.

2.4. 정보보호의도

디지털 헬스케어 서비스 시장이 지속적으로 성장하면서 디지털 헬스케어 서비스 제공자에 의해 지속적으로 의료정보 유출사고는 발생하고 있고, 이는 디지털 헬스케어 서비스 운영에 있어 심각한 문제라고 할 수 있다(박광하, 2021). 이러한 정보시스템 오남용에 대해 그간 ICT서비스 연구에서는 오남용 의도는 자신의 특정 목적을 이루고자 어떠한 불법적인 행위를 할지에 대한 개인의 의도로 정의되고 있다(Ajzen, 1991). 반면에 보호동기이론에서 보호 의도는 특정 위협에 대해 자신을 보호하고자 어떠한 행위를 할지 선택하는 의도로 정의되고 있다(Rogers, 1983). 따라서, 디지털 헬스케어 서비스 제공자의 정보보호의도는 정보의 부정적인 오남용과 긍정적인 보호라는 이요인적 관점에서 살펴볼 필요가 있다. 즉, 디지털 헬스케어 서비스 정보보호의도를 타인의 계정을 도용하거나 권한이 없는 서비스를 이용하는 등 부정적인 정보보호의도를 형성하는 유도통제의도와 정보 오남용을 하지 않고 스스로 정보를 보호하기 위한 노력을 하는 등 긍정적인 정보보호의도를 형성하는 자기방어의도로 나누어 살펴본다면 정보보호의도를 긍부정적인 측면 모두에서 살펴볼 수 있다고 할 수 있다(Ajzen, 1991; Lee et al., 2004).

Ⅲ. 연구가설

3.1. 위험평가과 정보보호의도

보호동기이론에서 위험평가는 심각성과 취약성으로 나뉘고, 심각성은 정보노출 시 발생하게 될 부정적인 결과에 대한 심각성을 인지하는 정도이고 취약성은 불법적인 접근이나 부당한 수집을 통해 발생할 수 있는 위험을 인지하고 있는 정보를 의미한다(Rippetoe & Rogers, 1987; Milne et al., 2000; Youn, 2005). 따라서, 심각성과 취약성을 고려하여 가정해 보면 디지털 헬스케어 서비스 제공자가 보안위협으로 인해 발생하는 위험에 대한 관심이나 인지가 높을수록 보안사고 발생 시 서비스 제공자 자신이 보안위협의 직간접적인 위험에 처할 수도 있다는 점을 더욱 더 알 수 있다고 있다고 생각해 볼 수 있다(김양훈·안병구, 2018). 즉, 디지털 헬스케어 서비스 제공자는 보안위협의 심각성을 느낄수록 서비스 제공자 자신이 보안위협에 취약하다고 느끼고 있다고 생각해볼 수 있다. 따라서, 아래의 가설을 통해 이를 확인하고자 한다.

가설1a: 디지털 헬스케어 서비스 제공자의 심각성은 취약성에 정(+)의 영향을 미칠 것이다.

디지털 헬스케어 서비스를 제공하면서 디지털 헬스케어 서비스 제공자는 보안위협의 결과에 대한 심각성과 자신이 항상 보안위협에 노출되어 있다는 취약성을 고려하며 디지털 헬스케어 서비스를 제공한다. 이는 보호동기이론에서 위험평가에 해당한다(Dinev & Hart, 2006). 즉, 디지털 헬스케어 서비스 제공자는 위험평가를 하면서 디지털 헬스케어 서비스를 불법적으로 이용하지 않으려는 태도를 취하게 된다고 예상해 볼 수 있는데, 이는 결과적으로 불법적인 오남용을 하지 않으려 하여 유도통제의도를 낮춘다고 생각해 볼 수 있다(송유진 외, 2019). 또한, 보안억제 관점에서는 디지털 헬스케어 서비스 제공자가 정보보호에 대해 이해를 많이 하고 있고 노력하고 있어서 실제 정보유출을 막을 수 있다고 믿는 경우에도 유도통제의도를 낮춘다고 생각해 볼 수 있다. 이에 따른 본 연구의 가설은 다음과 같다.

가설1b: 디지털 헬스케어 서비스 제공자의 심각성은 유도통제의도에 부(-)의 영향을 미칠 것이다.

가설1c: 디지털 헬스케어 서비스 제공자의 취약성은 유도통제의도에 부(-)의 영향을 미칠 것이다.

가설1d: 디지털 헬스케어 서비스 제공자의 반응효능감은 유도통제의도에 부(-)의 영향을 미칠 것이다.

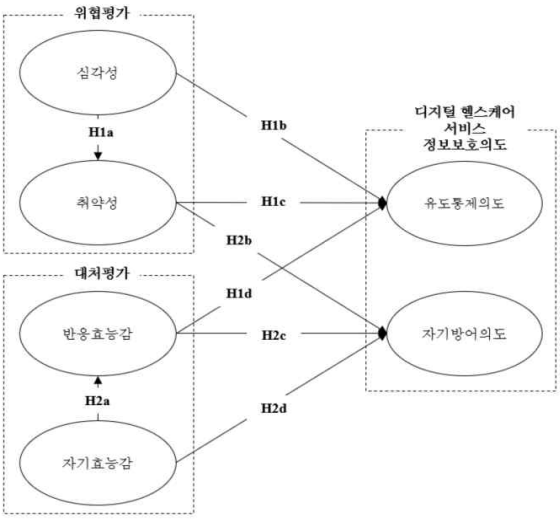
3.2. 대처평가와 정보보호의도

보호동기이론에서 대처평가는 자기효능감과 반응효능감으로 나뉘고, 자기효능감은 목적을 위해 가지고 있는 자신의 지식과 기술에 대한 믿음의 정도이고 반응효능감은 목적을 위해 부정적인 결과를 막기 위한 위험을 감소시킬 수 있다는 믿음의 정도를 의미한다(Compeau & Higgins, 1995; Workman et al., 2008; Bulgurcu et al., 2010). 따라서, 자기효능감과 반응효능감을 고려하여 생각해보면 디지털 헬스케어 서비스 제공자는 디지털 헬스케어 서비스를 제공하면서 다양한 보안기능을 경험하고 정보를 스스로 보호할 수 있다는 자기효능감을 통해 정보유출사고 발생 시 일정부분 처벌을 피할 수 있다는 생각을 할 수 있다(이난경·이종옥, 2015; 강민성 외, 2019). 이는 디지털 헬스케어 서비스 제공자가 느끼는 자기효능감이 높아지면 실제 정보유출에 잘 대비하고 있다는 신뢰인 반응효능감을 높여줄 것으로 생각해 볼 수 있다. 즉, 자신의 능력으로 다양한 보안위협을 해결할 수 있다는 자신감은 실제 보안위협에 대한 대처가 가능하다는 확신을 높여준다고 생각할 수 있을 것이다. 따라서, 아래의 가설을 통해 이를 확인하고자 한다.

가설2a: 디지털 헬스케어 서비스 제공자의 자기효능감은 반응효능감에 정(+)의 영향을 미칠 것이다.

마지막으로 디지털 헬스케어 서비스 제공자가 제공하고 있는 디지털 헬스케어 서비스가 보안위협에 노출될 수 있다고 생각하고, 이러한 대책의 효과를 신뢰하는 경우에 추가적인 정보보호 노력을 할 것이라고 예상해 볼 수 있다(Ng et al., 2009). 또한, 자신의 능력으로 이러한 보안위협을 해결할 수 있다는 자신감이 있는 경우 더욱 디지털 헬스케어 서비스의 불법적인 이용을 막으려는 의도가 생길 것으로 생각해볼 수 있다. 즉, 디지털 헬스케어 서비스 제공자의 취약성, 반응효능감, 자기효능감은 디지털 헬스케어 서비스 제공자가 스스로 불법적인 오남용을 막고자하는 의도인 자기방어의도에 긍정적인 영향을 줄 것이라고 생각해 볼 수 있다. 이에 따른 본 연구의 가설은 다음과 같다.

가설2b: 디지털 헬스케어 서비스 제공자의 취약성은 자기방어의도에 정(+)의 영향을 미칠 것이다.
가설2c: 디지털 헬스케어 서비스 제공자의 반응효능감은 자기방어의도에 정(+)의 영향을 미칠 것이다.
가설2d: 디지털 헬스케어 서비스 제공자의 자기효능감은 자기방어의도에 정(+)의 영향을 미칠 것이다.



<그림 1> 연구가설

Ⅳ. 실증분석

4.1. 연구변수

연구모형을 검증하기 위해 의료기관, 벤처기업 등의 디지털 헬스케어 서비스를 제공하는 디지털 헬스케어 서비스 제공자를 대상으로 설문을 실시하였다. 회수된 설문지 중 문항에 대한 응답이 누락되었거나 불성실한 답변으로 판단되는 6부를 제외하고 총 222부의 설문지를 본 연구를 위해 사용하였다. 실증분석을 위한 통계소프트웨어로는 SPSS 22.0과 AMOS 22.0을 사용하였으며 표본의 인구통계학적 특성과 일반적 특성을 분석하기 위하여 빈도분석을 실시하였다. 설문응답자들의 인구통계학적 특성을 살펴보면, 성별은 남성이 98명(44.1%), 여성이 124명(55.8%)으로 여성의 비율이 조금 높게 나타났다. 연령에 있어서는 30대가 90명(40.5%)로 가장 많이 차지하고 있고, 학력에 있어서는 대졸이 173명(77.9%)으로 가장 많이 차지하고 있는 것으로 나타났다. 마지막으로 설문응답자들의 직무분야는 헬스케어서비스와 ICT서비스에 주로 종사하는 것도 확인할 수 있다.

<표 1> 표본의 일반적 특성

구분		빈도(N)	비율(%)
성별	남성	98	44.1%
	여성	124	55.8%
연령	10대	10	4.5%
	20대	98	44.1%
	30대	86	38.7%
	40대 이상	28	12.6%
학력	고졸이하	28	12.6%
	대졸	173	77.9%
	대학원졸 이상	21	9.5%
직무 분야	헬스케어서비스직	108	48.6%
	ICT서비스직	73	32.9%
	일반사무직	24	10.8%
	관리직	17	7.7%

본 연구는 선행연구를 기반으로 도출된 정보보호의도에 영향 미치는 요인의 조작적 정의를 내리고 선행연구자들의 측정항목을 수정하여 연구문항을 구성하였다. <표 2>는 연구변수에 대한 개념적 정의 및 측정변수를 정의한 것이다.

<표 2> 연구변수의 개념적 정의

연구변수	개념적 정의	관련문헌
심각성	디지털 헬스케어 서비스를 제공하면서 보안위협으로 인해 발생하는 위험에 대한 인지의 정도	Rippetoe & Rogers, 1987; Milne et al., 2000; Workman et al., 2008
취약성	디지털 헬스케어 서비스를 제공하면서 보안위협에 노출될 위험에 대한 인지의 정도	Rippetoe & Rogers, 1987; Milne et al., 2000; Workman et al., 2008
반응효능감	디지털 헬스케어 서비스를 제공하면서 보안 대책의 효과에 대한 신뢰의 정도	Rippetoe & Rogers, 1987; Milne et al., 2000; Workman et al., 2008
자기효능감	디지털 헬스케어 서비스를 제공하면서 보안위협을 자신의 능력으로 해결할 수 있는 자신감의 정도	Compeau & Higgins,1995; Workman et al., 2008
유도통제의도	타인의 계정을 도용하거나 권한이 없는 디지털 헬스케어 서비스를 이용하려는 의도의 정도	Ajzen, 1991; Lee et al., 2004
자기방어의도	불법적인 디지털 헬스케어 서비스의 이용을 막으려는 의도의 정도	Ajzen, 1991; Lee et al., 2004

4.2. 요인분석

각 요인의 신뢰성과 타당성을 확인하기 위해 요인분석을 실시하였다. 탐색적 요인분석결과는 각 성분에 대한 요인분류는 0.7이상으로 모두 분류되었다. 이어서 각 요인의 신뢰성과 타당성을 확인하기 위해 요인분석을 실시하였다. 요인분석 결과, χ2(434.478, $p<0.000$), GFI=0.876, AGFI=0.891, NFI=0.932, CFI=0.946, TLI=0.945, RMSE=0.062 등의 적합지수를 보여 안정적인 결과를 도출하였으며, 비교적 높은 수치를 나타냈다. 결과적으로 전반적인 적합도에는 문제가 없음을 확인할 수 있었다. 신뢰성 검증은 일반적으로 구성신뢰도(Composite Reliability: CR)를 사용하며 0.7 이상은 신뢰성이 확보되었다고 할 수 있고, 집중타당성은 측정하고자 하는 항목과 잠재변수 간의 연관성으로 잠재변수의 평균분산추출(Average Variance Extracted: AVE) 값으로 알 수 있는데 일반적으로 0.7 이상을 요구한다. <표 3>에서 확인할 수 있는 것처럼 각 요인을 구성하는 측정문항들의 신뢰성과 타당성도 기준치 이상임을 확인할 수 있었다.

<표 3> 측정변수의 신뢰도와 타당성 분석결과

변수	심각성	취약성	반응 효능감	자기 효능감	유도 통제의도	자기 방어의도
AVE	0.866	0.870	0.842	0.857	0.918	0.867
C.R.	0.784	0.697	0.640	0.666	0.852	0.780

판별타당성 검증은 잠재변수의 AVE 제곱근 값과 잠재변수 간 상관계수 값을 비교하여 분석한다. 각 잠재변수의 AVE 제곱근의 값은 잠재변수 간 상관계수 값보다 크게 나타나야 하는데, 분석결과 <표 4>과 같이 AVE 제곱근 값이 종과 횡에 있는 잠재변수 간의 상관계수 값보다 더 높으므로 판별 타당성의 존재도 확인할 수 있었다.

<표 4> 판별타당성 검증결과

ρ^2	1	2	3	4	5	6
심각성	0.749					
취약성	0.450	0.756				
반응효능감	0.480	0.195	0.708			
자기효능감	0.388	0.124	0.502	0.734		
유도통제의도	-0.254	-0.105	-0.072	0.090	0.842	
자기방어의도	0.314	0.263	0.583	0.499	0.032	0.751

4.3. 분석결과

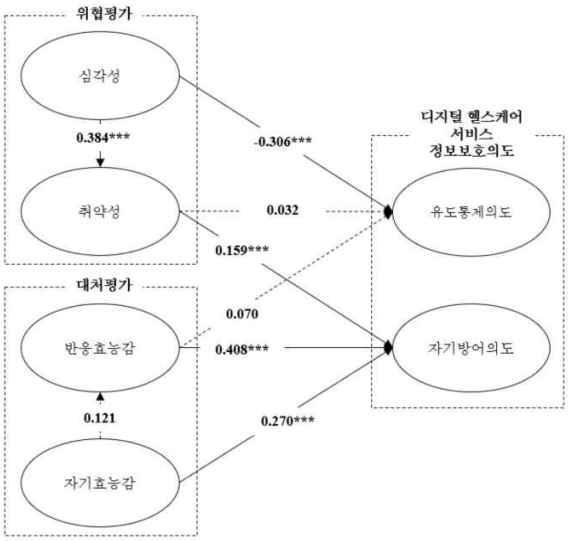
요인분석을 통해 요인의 신뢰성과 타당성이 검증되었으므로 연구모형의 적합성에 대한 검증을 실시하였다. 분석결과 χ2(727.593, $p<0.000$), GFI=0.798, CFI=0.912, NFI=0.891, TLI=0.879, RMSE=0.090, 등의 적합지수를 보였다. 일부 지수가 보수적인 수준(0.9이상)에 미치지는 못하지만, 보수적인 수준에 근접해 있고 적합도 지수에 절대적인 기준은 없다는 점 등을 고려할 때 연구모형의 적합도는 신뢰할 만하다고 할 수 있다. 또한 기초모형에 대한 제안모형의 전반적인 적합지수(NFI)가 높은 수준(0.891)이며, 기초모형이 평균과 제약이 없음을 가정한 제안모형과 비교적합지수(CFI)가 0.912로 높은 수준이며, 비표준화된 비교적합지수(TLI)도 0.879수준으로 높은 결과를 보이므로 모형은 비교적 적합하다고 할 수 있다. 따라서, 본 연구모형의 결과는 신뢰할 만한 수준에 있다고 할 수 있다.

구조방정식을 이용한 각 가설에 대한 검정결과는 <표 5>와 같다. H1의 각 경로계수는 H1a(0.384, $p<0.01$), H1b(-0.306, $p<0.01$), H1c(0.032, 기각), H1d(0.070, 기각)로 디지털 헬스케어 서비스 제공자가 느끼는 심각성이 취약성에 유의한 영향을 미치고, 디지털 헬스케어 서비스 제공자의 유도통제의도에는 심각성이 유의한 영향을 미치고 있음을 확인할 수 있다. 이는 디지털 헬스케어 서비스 제공자는 보안위협에 대한 심각성을 느끼는 경우 디지털 헬스케어 서비스에서 규정하고 있는 접근권한 등에 대한 준수가 잘 이뤄질 것이라는 점을 시사한다. H2의 경로계수는 H2a(0.112, 기각), H2b(0.159, $p<0.01$), H2c(0.408, $p<0.01$), H2d(0.270, $p<0.01$)로 디지털 헬스케어 서비스 제공자는 보안위협에 대한 대처능력이 있다고 생각할수록 정보보호에 대한 이해도도 높고 디지털 헬스케어 서비스에 대한 보안대책에 대한 신뢰를 가지고 스스로 불법적인 이용을 막으려 하는 등 보안위협에 적극적으로 대응할 것이라는 점을 시사한다. 또한, 보안위협에 대한 취약성을 인지하는 경우에도 보안대책 마련에 적극적으로 참여할 것으로 생각된다.

<표 5> 연구모형의 가설검증 결과

가설	경로	표준화 계수	SE	CR	*p*	결과
H1a	심각성 → 취약성	0.384	0.088	4.747	0.000***	채택
H1b	심각성 → 유도통제의도	-0.306	0.064	-3.455	0.000***	채택
H1c	취약성 → 유도통제의도	0.032	0.050	0.433	0.665	기각
H1d	반응효능감 → 유도통제의도	0.070	0.068	0.974	0.330	기각
H2a	자기효능감 → 반응효능감	0.121	0.052	1.526	0.127	기각
H2b	취약성 → 자기방어의도	0.159	0.061	2.676	0.007***	채택
H2c	반응효능감 → 자기방어의도	0.408	0.109	5.703	0.000***	채택
H2d	자기효능감 → 자기방어의도	0.270	0.068	4.022	0.000***	채택

** p<0.05, ** p<0.01, *** p<0.001*



<그림 2> 연구결과

Ⅴ. 결론

의료정보는 유출되는 경우 2차로 정신적인 피해를 줄 수 있는 매우 민감한 정보라고 할 수 있고, 디지털 헬스케어 서비스 제공자의 낮은 보안의식에 따른 정보유출사고가 지속적으로 증가하고 있는 추세로 디지털 헬스케어 서비스 제공자의 정보보호의도에 대한 이해가 매우 중요하다고 할 수 있다. 그러나 그간 디지털 헬스케어 서비스 제공자 또는 정보 취급자의 정보보호에 대한 연구는 주로 보안정책의 개선, 보안시스템의 성능을 향상시키는데 주요한 관심을 가진 반면, 디지털 헬스케어 서비스 제공자의 정보보호의도에 영향을 주는 요인에는 큰 관심을 가지지 못하였다. 따라서, 본 연구는 디지털 헬스케어 서비스 제공자의 이용환경에 주안점을 두고 정보보호의도에 영향을 주는 요인의 확인을 통한 시사점을 살펴보았다. 즉, 본 연구는 보호동기이론을 활용한 연구모형을 고안하여 어떠한 선행요인이 디지털 헬스케어 서비스 제공자의 유도통제의도와 자기방어의도를 유발시키고, 정보보호의도의 형성에 어떠한 영향을 미치는지 확인하였다. 따라서, 본 연구는 정보유출 사고가 주로 디지털 헬스케어 서비스 제공자에 의해 발생한다는 점을 착안하여, 디지털 헬스케어 서비스 제공자가 느끼는 정보보호에 보다 실질적인 도움을 주는 연구결과를 도출했다는 점에서 기존 연구의 한계를 극복했다고 할 수 있다.

본 연구를 통해 디지털 헬스케어 서비스 제공자가 보안위협에 대한 심각성을 인지하고 디지털 헬스케어 서비스의 정보보안 기능을 신뢰하며 잘 활용할 수 있다는 자신감이 있을 때 정보보호의도가 높아진다는 점을 확인하였다. 따라서, 본 연구결과를 통한 디지털 헬스케어 서비스를 운영하고 있는 벤처기업을 위한 실무적 의의는 다음과 같다. 첫째, 보안정책을 아무리 정교하게 수립하여도 헬스케어 서비스 제공자가 보안위협에 대한 결과를 명확하게 인지하고 있지 못하면 정보유출사고에 대한 심각성과 보안대책에 대한 신뢰, 자신감이 적어진다. 이는 디지털 헬스케어 서비스의 운영을 위해 수립한 보안정책 뿐만 아니라 보안위협의 결과를 디지털 헬스케어 서비스 제공자가 명확하게 인지할 수 있도록 하여야 한다는 점을 시사한다. 즉, 실제 피해사례 중심의 교육이나 공지를 통한 안내 등을 통해 보안위협의 결과를 보다 직관적으로 이해시켜야만 한다는 것을 의미한다. 둘째, 제공하고 있는 디지털 헬스케어 서비스의 보안수준에 대한 만족감은 디지털 헬스케어 서비스 제공자의 정보보호의도에 대한 자신감을 높여주고, 이를 통해 서비스 제공자의 자기방어의도가 높아진다. 즉, 다뤄지는 헬스케어 정보에 대한 보안노력을 지속적으로 하고 신뢰할 수 있는 보안시스템을 도입하였다는 점을 디지털 헬스케어 서비스 제공자가 늘 인지할 수 있도록 노력해야만 한다고 할 수 있다. 또한, 반응효능감이 대처평가의 주요한 요인인데 이는 보안시스템에 대한 만족이 보안대책의 효과에 대한 신뢰를 형성시켜, 디지털 헬스케어 서비스 제공자 스스로 정보보호에 동참하고자 하는 동기를 유발한다고 할 수 있다. 마지막으로 디지털 헬스케어 서비스 제공자의 불법적인 오남용 의도인 유도통제의도에 심각성이 주요한 선행요인이라는 점은 디지털 헬스케어 서비스 제공자들은 보안위협의 결과로 발생하는 위협에 대해서는 잘 알고 있지만, 실제 디지털 헬스케어 서비스 제공자들이 자신에게는 이러한 위협이 발생하지 않을 것이라고 생각하고 있다는 점을 시사한다. 이는 디지털 헬스케어 서비스를 운영하는 벤처기업들은 디지털 헬스케어 서비스 제공자에게 정보유출에 따라 발생하는 다양한 위협과 돌아올 책임에 대해 명확하게 안내하여 언제든지 자신에게도 보안위협에 따른 피해가 발생할 수 있음을 인지시켜야만 한다고 할 수 있다.

본 연구를 통해 도출할 수 있는 디지털 헬스케어 서비스를 운영하는 벤처기업이 디지털 헬스케어 서비스 제공자의 정보보호의도를 높일 수 있는 전략은 다음과 같다. 첫째, 디지털 헬스케어 서비스 제공자가 보안정책을 명확하게 이해할 수 있고, 정보유출로 인해 발생하는 다양한 위협과 결과에 따른

책임을 인지할 수 있도록 보안의식에 대한 공지, 디지털 헬스케어 서비스 제공자가 쉽게 이해할 수 있는 콘텐츠 제공에 힘써야 할 것이다. 최근 발생하는 상당수의 정보유출사고 디지털 헬스케어 서비스 제공자의 부주의나 오남용에 의한 결과로 이러한 정보유출사고를 미연에 방지하기 위해서는 디지털 헬스케어 서비스 제공자를 위한 보안의식을 높일 수 있는 다양한 콘텐츠 제공이 매우 중요하다고 할 수 있다. 둘째, 디지털 헬스케어 서비스를 운영하는 벤처기업은 타 분야의 벤처기업에 비해 보다 높은 수준의 보안시스템에 대한 투자가 필요하다. 디지털 헬스케어 서비스 제공자가 보안시스템의 필요성을 느끼고 만족하게 사용하고, 쉽게 사용할 수 있다고 생각하는 자신감은 정보보호의도를 높이는데 직접적인 요인이다. 즉, 디지털 헬스케어 서비스 제공자가 신뢰할 수 있고, 만족할 수 있는 수준의 보안시스템에 대한 투자가 이뤄져야만, 디지털 헬스케어 서비스 제공자의 정보보안에 대한 자신감을 높여줄 수 있다고 할 수 있다.

Ⅵ. 한계점

본 연구를 통해 디지털 헬스케어 서비스 제공자의 정보보호의도에 미치는 요인을 확인할 수 있었다. 하지만, 디지털 헬스케어 서비스 제공자의 정보보호의도에 미치는 요인은 보다 광범위하고, 디지털 헬스케어 서비스는 매우 다양하다. 따라서, 본 연구의 한계점은 다음과 같다. 첫째, 본 연구는 정보보호의도에 미치는 요인을 보호동기이론을 기반으로 위험평가와 대체평가로 구분하여 설명하였는데, 디지털 헬스케어 서비스의 특성을 고려하여 이를 더 세분화하거나 보다 많은 요인을 포함하여 분석할 필요가 있다. 둘째, 설문의 대상이 주로 한국의 30대 위주로 되어 있어 분석결과의 일반화가 어렵고, 특정 국가와 집단의 특징에 따른 무형적인 요인에 대한 설명력이 누락되었다고 할 수 있다. 때문에, 향후 다양한 집단에 본 방법론을 적용해 보거나, 집단의 특성을 반영할 수 있는 선호요인을 포함하여 연구되어야 할 필요성이 있다. 따라서, 위에서 제시한 한계점을 고려하여 연구한다면 보다 구체적으로 벤처기업이 활용할 수 있는 디지털 헬스케어 서비스 제공자의 정보보호의도에 영향을 미치는 요인을 찾아내어, 디지털 헬스케어 서비스를 운영하는 벤처기업의 시장지배전략을 더욱 정교하게 수립할 수 있도록 도와줄 수 있을 것이라고 생각한다.

REFERENCE

강민성·김태성·김택영(2019). 정보보호 교육이 청소년의 정보보호 실천에 미치는 영향. *Journal of Information Technology Applications & Management*, 26(2), 27-40.

권혁준·김협·최재원(2018). 개인 의료정보 보호를 위한 블록체인 적용 방안: 프라이빗 블록 스킴을 중심으로. *지식경영연구*, 19(4), 119-131.

김강한(2016). 개인건강정보보호에 관한 헌법적 고찰: 공공영역에서의 개인건강정보보호를 중심으로. *아주법학*, 10(2), 1-40.

김양훈·안병구(2018). 의료융합 환경에서 수용성을 고려한 비용 효율적 보안체계구축 방안 연구: 중소의료기관을 중심으로. *융합보안논문지*, 18(5), 75-81.

김영수·정재진(2019). E 헬스케어 비즈니스모델에 관한 연구: 비즈니스생태계 접근 중심으로. *벤처창업연구*, 14(1), 167-185.

김영신(2021.10.27.). *2020년 2월, 의료법 개정 개정 후 총 25개 병원 해킹시도…종합병원급 이상 8곳*. 메디컬월드뉴스, http://medicalworldnews.co.kr/news/view.php?idx=1510945760.

김호다·주애란(2021). 서비스 디자인 관점에서 본 스마트 헬스케어의 선행 조건: 고령자 경험 사례를 중심으로. *Journal of Information Technology Applications & Management*, 28(3) 49-58.

박광하(2021.10.26.). *진료정보 보호 위한 의료법 개정안 발의*. 정보통신신문, http://www.koit.co.kr/news/articleView.html?idxno=90215.

박민정·채상미·이명준(2018). 개인정보보호법제 관점에서 본 블록체인의 법적 쟁점: Gdpr 및 국내 개인정보보호법을 바탕으로. *Journal of Information Technology Applications & Management*, 25(2), 133-146.

박아름·송재민·이새봄(2020). 빅데이터 기술을 활용한 헬스케어 서비스 동향 분석. *한국컴퓨터정보학회논문지*, 25(4), 149-156.

소현정·곽기영(2021). 모바일 헬스 앱 사용의도 동기요인: 조절초점 성향과 프라이버시계산이론을 중심으로. *지식경영연구*, 22(2), 33-53.

송유진·김민희·최세정(2019). 쇼핑 챗봇에 대한 소비자 반응 연구: 에이전트와 메시지 유형 효과를 중심으로. *한국 Hci 학회 논문지*, 14(2), 71-81.

안정민(2021). 디지털 헬스케어 산업과 원격의료 산업의 경제적 파급효과 비교분석. *E-비즈니스연구*, 22(5), 15-25.

양재민·현병환·옥준우(2020). 스마트폰 사용행태 분석과 헬스케어 어플리케이션의 기능 및 사용의도에 대한 연구. *벤처창업연구*, 15(4) 303-315.

엄혜미(2021). 데이터 통합 모델 기반 e-transformation 전략: 장기요양기관 사례. *Journal of Information Technology Applications & Management*, 28(3), 23-30.

윤은준(2012). U-헬스케어 서비스에서의 정보보호 기술 동향. *한국통신학회지*, 29(10), 55-65.

이난경·이종옥(2015). 중소형 병원의 클라우드 병원정보시스템 서비스 체계에 관한 연구. *한국전자거래학회지*, 20(3), 89-112.

이성경·박상철·서은희·고준(2020). 원격의료 서비스 실행과정에서의 이해관계자 이슈 분석: 근거이론 접근. *지식경영연구*, 21(4), 1-19.

이한주(2014). 개인의료정보보호법 제정의 필요성과 입법방향. *한국의료법학회지*, 22(1), 177-208.

임성훈·김용태(2015). 헬스케어산업 관점에서 본 린스타트업 적용 사례연구: ㈜휴메딕스 사례를 중심으로. *벤처창업연구*, 10(3), 99-109.

장철호·차윤호(2021). 개인정보보호 활동 결정요인 연구: 개인정보처리자를 중심으로. *정보화정책*, 28(1), 64-76.

정준호·김정숙(2015). U-헬스케어 (healthcare) 환경에 따른 의료정보 보안 이슈. *한국멀티미디어학회지*, 19(3), 36-41.

함민정(2022.2.25.). *20만명 의료정보 털린 대형병원…"통지가 끝?" 피해자들 분노*. 중앙일보, https://www.joongang.co.kr

/article/25051054#home.

Agarwal, R., Gao, G., DesRoches, C., & Ashish. K. J.(2010). The digital transformation of healthcare: Current status and the road ahead. *Information Systems Research*, 21(4), 796-809.

Ahn, J. M.(2021). Comparative Analysis of the Economic Ripple Effect of the Digital Healthcare Industry and the Telemedicine Industry. *The e-Business Studies*, 22(5), 15-25.

Ajzen, I.(1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 50(2), 179-211.

Anderson, C. L., & Agarwal, R.(2011). The digitization of healthcare: Boundary risks, emotion, and consumer willingness to disclose personal health information. *Information Systems Research*, 22(3), 469-490.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I.(2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, 34(3), 523-548.

Choi, H. S., Lee, W. S., & Sohn, S. Y.(2017). Analyzing research trends in personal information privacy using topic modeling. *Computers & Security*, 67, 244-253.

Compeau, D. R., & Higgins, C. A.(1995). Computer self-efficacy: Development of a measure and initial test. *MIS Quarterly*, 19(2), 189-211.

Dinev, T., & Hart, P.(2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, 17(1), 61-80.

Edwards, W.(1954). The theory of decision making. *Psychological Bulletin*, 51(4), 380-417.

Gonsalves, J.(2018). The necessity for federal organizations to ensure proper privacy and security compliance of mobile health care applications. *Journal of High Technology*, 19(1.5), 251-278.

Gritzalis, D., & Lambrinoudakis, C.(2004). A security architecture for interconnecting health information systems. *International Journal of Medical Informatics*, 73(3), 305-309.

Guadarrama, A.(2018). Mind the gap: Addressing gaps in HIPAA coverage in the mobile health apps industry. *Houston Law Review*, 55(4), 999-1025.

Ham, M. J.(2022.2.25.). *A large hospital with 200,000 medical information stolen. "Is the notice over?" victims' anger.* The JoongAng, https://www.joongang.co.kr/article/25051054#home.

Hurson, A. R., Ploskonka, J. A., Jiao, Y., & Haridas, H.(2004). Security issues and solutions in distributed heterogeneous mobile database systems. *Advances in Computers*, 61, 107-198.

Jang, C. H., & Cha, Y. H.(2021). A Study on the Determinants of Personal Information Protection Activities: With a Focus on Personal Information Managers. *Informatization Policy*, 28(1), 64-76.

Jung, J. H., & Kim, J. S.(2015). Medical information security issues according to the U-health care environment. *Journal of Korea Multimedia Society*, 19(3), 36-41.

Kang, M. S., Kim, T. S., & Kim, T. Y.(2019). Effects of Information Security Education on the Practice of Information Security for the Youth. *Journal of Information Technology Applications & Management*, 26(2), 27-40.

Kim, H. D., & Joo, A. R.(2021). Prerequisites on Smart Healthcare in the Perspective of Service Design: Focusing on the Elderly Experience Case. *Journal of Information Technology Applications & Management*, 28(3) 49-58.

Kim, K. H.(2016). A Constitutional Study on the Protection of Personal Health Information: With the focus on the protection of personal health information in the public sector. *Ajou Law Review*, 10(2), 1-40.

Kim, Y. H., & Ahn, B. G.(2018). A Study on the Cost-Effective Security System for SME Hospital Acceptability in Convergence Medical Environment. *Journal of Convergence Security*, 18(5), 75-81.

Kim, Y. S., & Jung, J. J.(2019). A Study on e-Healthcare Business Model: Focusing on Business Ecosystem Approach. *Asia-Pacific Journal of Business Venturing and Entrepreneurship*, 14(1), 167-185.

Kim, Y. S.(2021.10.27.). *In February 2020, after the revision of the medical law, a total of 25 hospitals were hacke d… 8 general hospitals or higher.* Medical World News. *http://medicalworldnews.co.kr/news/view.php?idx=151*0945760.

Kokolakis, S.(2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, 64, 122-134.

Kwon, H. J., Kim, H., & Choi, J. W.(2018). A Blockchain Application for Personal health information: Focusing on Private Block Scheme. *Knowledge Management Review*, 19(4), 119-131.

Lee, H. J.(2014). The Legislation on the Personal Medical Information Protection Law. *Korean Journal of Medicine and Law*, 22(1), 177-208.

Lee, N. K., & Lee, J. O.(2015). A Study on the Architecture of Cloud Hospital Information System for Small and Medium Sized Hospitals. *The Journal of Society for e-Business Studies*, 20(3), 89-112.

Lee, S. K., Park, S. C., Seo, E. H., & Koh, J.(2020). An Analysis of Stakeholder Issues in the Implementation of Telemedicine Services: Based on Grounded Theory. *Knowledge Management Review*, 21(4), 1-19.

Lee, S. M., Lee, S. G., & Yoo, S.(2004). An integrative model of computer abuse based on social control and general deterrence theories. *Information & Management*, 41(6), 707-718.

Lim, S. H., & Kim, Y. T.(2015). Lean Startup Application Study in the Healthcare Industrial point of View: The Case of Humedix Corporation. *Asia-Pacific Journal of Business Venturing and Entrepreneurship*, 10(3), 99-109.

Milne, S., Sheeran, P., & Orbell, S.(2000). Prediction and intervention in health related behavior: A meta-analytic review of protection motivation theory. *Journal of Applied Social Psychology*, 30(1), 106-143.

Ng, B., Kankanhalli, A., & Xu, Y. C.(2009). Studying users' computer security behavior: A health belief perspective.

Decision Support Systems, 46(4), 815-825.

Park, A. R., Song, J. M., & Lee, S. B.(2020). Healthcare service analysis using big data. *Journal of The Korea Society of Computer and Information*, 25(4), 149-156.

Park, G. H.(2021.10.26.). *Proposed amendment to the Medical Act to protect medical information.* Korea Information and Communication Newspaper, https://www.koit.co.kr/news/articleView.html?idxno=90215.

Park, M. J., Chai, S. M., & Lee, M. J.(2018). Legal Issues of Blockchain in Personal Information Protection: Based on GDPR and Personal Information Protection Act. *Journal of Information Technology Applications & Management*, 25(2), 133-146.

Peppard, J., & Ward, J.(2016). *The strategic management of information systems: Building a digital strategy*. John Wiley & Sons.

Rippetoe, P. A., & Rogers, R. W.(1987). Effects of components of protection-motivation theory on adaptive and maladaptive coping with a health threat. *Journal of Personality and Social Psychology*, 52(3), 596.

Rogers, R. W.(1983). *Cognitive and psychological processes in fear appeals and attitude change: A revised theory of protection motivation*. Social Psychophysiology.

So, H. J., & Kwahk, K. Y.(2021). Motivational Factors Affecting Intention to Use Mobile Health Apps: Focusing on Regulatory Focus Tendency and Privacy Calculus Theory. *Knowledge Management Review*, 22(2), 33-53.

Solove, D. J., & Schwartz, P.(2014). *Information privacy law*. Wolters Kluwer.

Song, Y. J., Kim, M. H., & Choi, S. J.(2019). A Study on Consumers' Responses to Shopping Chatbot: The Effects of Agent and Message Types. *Journal of the HCI Society of Korea*, 14(2), 71-81.

Um, H. M.(2021). e-Transformation Strategy of Data Integration Model: Long-Term Care Agency Case. *Journal of Information Technology Applications & Management*, 28(3), 23-30.

Vance, A., Siponen, M., & Pahnila, S.(2012). Motivating IS security compliance: Insights from habit and protection motivation theory. *Information & Management*, 49(3-4), 190-198.

Workman, M., Bommer, W. H., & Straub, D.(2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior*, 24(6), 2799-2816.

Wu, L., Li, J., & Fu, C.(2011). The adoption of mobile healthcare by hospital's professionals: An integrative perspective. *Decision Support Systems*, 51(3), 587-596.

Yang, J. M., Hyun, B. H., & Ok, J. W.(2020). A Study on the Function and Intention of the Health Care Application in the Analysis of Smartphone Usage Behavior. *Asia-Pacific Journal of Business Venturing and Entrepreneurship*, 15(4), 303-315.

Yoon, U. J.(2012). Information security technology trend in u-healthcare service. *Information & Communications Magazine*, 29(10), 55-65.

Youn, S.(2005). Teenagers' perceptions of online privacy and coping behaviors: A risk-benefit appraisal approach. *Journal of Broadcasting & Electronic Media*, 49(1), 86-110.

A Study on the Information Protection Intention of Digital Healthcare Service Providers

Chang-Gyu, Yang*

Abstract

This study investigates the IPI (Information Protection Intention) of DHS (Digital Healthcare Service) providers by introducing PMT (Protection Motivation Theory). This study examines the effects of protection motivation, such as threat appraisal and coping appraisal, on IPI, such as ICI(Induction Control Intention) and SDI(Self Defense Intention). The research model, based on the PMT, adopted severity, vulnerability, reaction efficacy and self-efficacy as independent variables. The research model was validated through quantitative research, a survey of 222 DHS providers in South Korea, using structural equation modeling. The results show that (1) a clear awareness of the consequences of security threats increases the understanding of DHS providers on the severity of closure of healthcare information, and thus may decreases abuse of DHS by providers; (2) user confidence and satisfaction on the security system may make them be confident that they can handle the closure of healthcare information by themselves; and (3) although DHS providers are realizing the consequences of closure of healthcare information, they think that they are unlikely to encounter such situations. As a result of this study, venture companies that provide DHS need to provide contents that can continuously increase providers' security level in order to increase providers' information protection intention. It suggests that IPI is important through trust of healthcare service providers.

KeyWords: Information protection intention, Digital healthcare service, Protection Motivation Theory, Protect healthcare information

* First Author, Department of e-Business, Ajou University, cozlove@ajou.ac.kr