목적: Lilly 또는 그 대리인이 제공하는 정보를 취급하는 경우에 대한 주요 메시지.

업무 취지상, 이러한 정보에는 당사가 비즈니스 목적으로 사용하는 기밀 정보와 개인 정보가 모두 포함됩니다. 개인 정보에는 단독으로 또는 다른 정보와 조합하여 사용할 경우 개인을 특정할 수 있는 모든 정보가 포함됩니다. 기밀 정보는 비밀공개 당사자가 기밀 또는 독점 정보로 간주하는 모든 정보로 정의됩니다.

검토 후 현재 귀하의 조직에서 Lilly 또는 그 대리인이 제공하는 정보를 취급하고 있거나 향후 취급하게 될 각 개인에게 전파하십시오.

이것이 중요한 이유는 무엇입니까?

- 귀사와 귀사의 직원은 Lilly의 소중한 협력자이며, 귀사와 귀사의 직원이 수행하는 조치는 정보 침해에 대한 최선의 1차 방어선입니다.
- 정보 보호는 Lilly와 Lilly를 이용하는 환자에게 매우 중요한 사안입니다.

NIST Cybersecurity Framework를 비롯한 업계 모범 사례를 참고한 다음, 주요 메시지를 현재 관행에 통합하여 정보 취급에 따르는 위험을 지속적으로 낮춰야 합니다.

일반:

- 반드시 필요한 경우가 아닌 한, 정보가 수록된 문서의 전자 사본 또는 하드카피 사본을 중복하여 만들지 마십시오.

전자 데이터 저장소:

- 정보가 포함된 전자 파일은 안전하게 저장해야 합니다.
    - Lilly 또는 그 대리인이 제공하는 정보에 대해 이전에 공개하거나 Lilly와 합의하지 않은 외부 저장소 또는 클라우드 서비스를 귀사에서 활용하는 경우 Lilly 담당자와 협조하십시오.
    - 정보가 포함된 전자 파일에 대한 액세스는 그 정보를 알아야 할 사람을 대상으로 필요한 범위 내에서 필요한 시간 동안만 부여되어야 합니다(최소 권한).
    - 민감도를 기준으로 액세스를 검토해야 합니다. 여기에는 귀하 및 귀하의 하도급 업체가 관리하는 저장소 위치가 포함됩니다.
    - 해당 개인이 퇴사하거나 업무상 더 이상 정보에 액세스할 필요가 없어지면 적시에 비활성화해야 합니다.
- Lilly의 승인 없이 다음과 같은 장소에 정보를 저장해서는 안 됩니다.
    - 외장 하드 드라이브 또는 USB 등의 이동식 저장 장치
    - 랩톱 또는 iPad 등 직원의 개인용 장치

전자 데이터 전송:

- 정보가 포함된 전자 파일은 안전하게 전송해야 합니다(중요도에 상응). 사용할 전송 방법은 Lilly 담당자와 협의하십시오.
- 보내기 전에 받는 사람의 이메일 주소를 확인하고, 업무상 정보를 알 필요가 있는 사람에게만 보내십시오.
- 다음을 통해 정보를 전송하면 안 됩니다.
    - Lilly의 승인을 받지 않은 외장 하드 드라이브 또는 USB와 같은 외부 저장 장치
    - 개인 이메일

안전한 정보 취급을 위한 비즈니스 규칙

인쇄:

- 가정용/개인용 프린터를 사용하거나 공공 장소에서 정보를 인쇄하는 것은 지양해야 합니다. 가정 또는 외부에서 인쇄해야 하는 경우, 케이블 또는 무선 네트워크를 통해 랩톱 또는 기타 승인된 장치(예: iPad)를 프린터에 연결하십시오.

화상 회의:

- 비즈니스용 Skype, Cisco WebEx 또는 Citrix GoToMeeting 을 사용하여 수행해야 합니다. 이 중 하나를 사용할 수 없는 경우 Lilly 담당자에게 문의하십시오.
- 온라인 회의는 Lilly 의 공지 및 사전 승인 없이 녹화되지 않습니다.
- 정보에 대해 논의할 때는 주변 환경에 주의를 기울이고 조심하십시오.

물리적 보안:

- 안전한 업무 공간 유지:
    - 컴퓨터에서 떠나 있을 때는 항상 컴퓨터에 액세스하지 못하도록 잠가 두십시오.
    - 퇴근할 때 랩톱 및 iPad 는 잠금 장치가 있는 캐비닛에 넣거나 케이블 잠금장치로 고정하거나 가지고 가야 합니다.
    - 퇴근할 때 책상, 캐비닛 및 라커/사무실을 잠그십시오.
    - 프린터에 하드카피를 남겨두지 마십시오.
    - 가능한 경우 우편, 배송 또는 팩스보다는 항상 협의된 전자 전송 방법을 사용하십시오.
    - 정보를 안전하게 폐기하십시오(예: 파쇄).

문자 메시지:

- Lilly 또는 그 대리인이 제공한 정보는 문자 메시지에 포함되지 않음

정보 보안 사고 보고:

- 정보 보안 사고가 발생하는 경우 Lilly 관계 관리자 또는 후원자에게 연락하고, 내부인 경우 Ethics and Compliance Hotline 을 통해, 외부인 경우 Lilly 액세스 또는 EthicsPoint 를 통해 우려 사항을 보고하십시오. 사고는 다음을 포함하나 이에 국한되지 않습니다.
    - 정보가 포함된 이메일이 의도하지 않은 수신인에게 우발적으로 발송됨.
    - 정보가 포함된 랩톱, 하드 드라이브 또는 이동식 저장 장치의 분실이나 도난.
    - 정보에 액세스할 수 있는 하도급 업체가 회사에 사고를 알림.
    - 랜섬웨어
      아래와 비슷한 화면이 표시되는 경우 다음 단계에 따르면 위험을 줄일 수 있습니다.
        - 네트워크 케이블을 분리하거나 무선 어댑터를 비활성화합니다.
        - 최대 절전 모드를 실행합니다.

안전한 정보 취급을 위한 비즈니스 규칙

피싱 주의!

- 피싱은 악의적인 의도를 가진 외부 침입자가 신뢰할 수 있는 주체로 가장하여 정보를 획득하기 위해 사용하는 수단입니다. 이메일의 확인되지 않은 첨부파일이나 링크를 클릭하면 컴퓨터와 전체 네트워크가 감염될 수 있습니다.

- 피싱 시도는 예기치 못한 메시지 형태로 나타나며, 거의 항상 다음과 같은 요소를 포함합니다.

    - 긴급한 행동 요구(예: 신용 카드 결제 연체).
    - 시간적 요소(예: 무언가가 2 일 내에 만료됨).
    - 결과(예: 이 문제를 해결하지 않으면 나쁜 일이 일어날 것임).
    - 엉성한 문법 또는 맞춤법 오류.
    - 또한 링크 또는 첨부파일 등을 "클릭"하는 요소가 항상 포함됩니다.

- 동작을 **멈**추고 **조**사하십시오. 직감을 사용하십시오. 이메일이 의심스럽다면 잠시 시간을 내서 메시지를 자세히 살펴보십시오. 기다리던 이메일이 아닌 경우 링크를 클릭하거나 첨부파일을 열지 마십시오.

- Lilly 이메일 주소를 사용하는 개인은 Lilly 의 공식 교육용 피싱 프로그램에 참여하게 됩니다. 반복적으로 클릭하는 사람의 이름은 제 3 자에게 전달되며, 후속 조치로 지도를 받게 될 수 있습니다. Lilly 공식 피싱 교육 프로그램과 관련하여 궁금한 점은 Lilly 담당자에게 문의하십시오. Lilly 이메일에서 의심스러워 보이는 메시지의 링크를 클릭하거나 첨부파일을 연 경우 Operation Screen Door 를 통해 보고하십시오.

궁금한 점 또는 우려 사항이 있는 경우:

- 위에 언급된 항목과 관련하여 궁금한 점 또는 우려 사항이 있는 경우 Lilly 담당자에게 문의하십시오.
- 이 정보는 공급자 포털의 Protect Lilly 아래에서도 찾을 수 있습니다.

15 July 2017