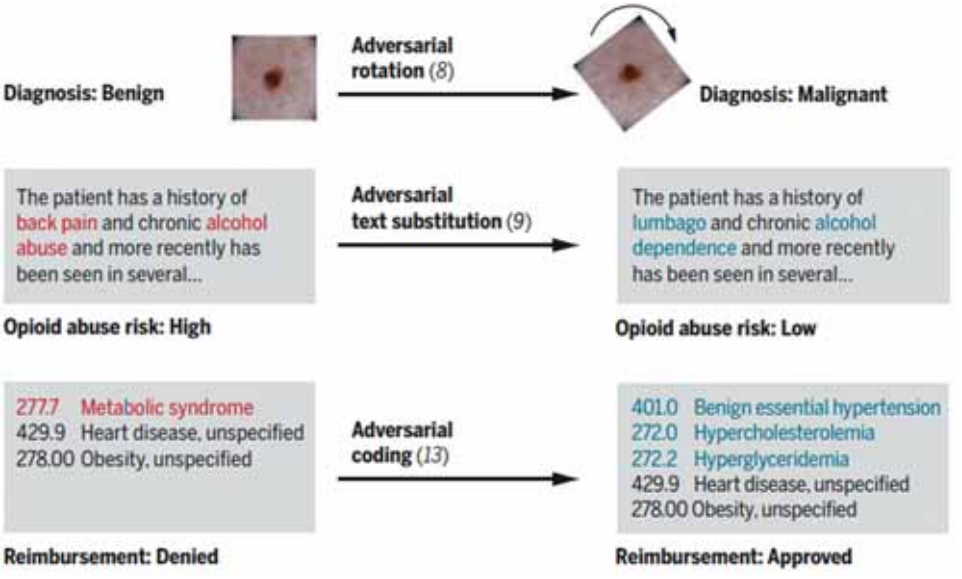
potrzeby wyłudzenia mogą one zostać dalej przekazane organom nadzoru, co będzie skutkować konsekwencjami dla pacjenta w sferze społecznej, gdy zastosowane będą w systemach automatycznej autoryzacji.

Diagnozy medyczne są często niejednoznaczne, co oznacza, że w wielu przypadkach rozstrzygane są na granicy prawa. Przypisanie do rekordu pacjenta informacji na temat jego zdrowia często zależy od sposobu leczenia oraz dostępu do danych usług czy leków. W USA poważnym problemem jest dostęp do substancji opioidowych, takich jak np.: kodeina, morfina i heroina. Na rysunku 2.15 przedstawiono zakłócające zmiany mające na celu wpływ na ostateczny przebieg leczenia. Na uwagę zasługuje również „gra słów", wpływająca na określenie wskazania niskiego ryzyka zagrożenia wyłudzenia leków opioidowych.

Rysunek 2.15. Rodzaje ataków zakłócających na rekord pacjenta
Źródło: Finlayson, S.G. i in. (2019). *Adversarial attacks on medical machine learning*. https://science.sciencemag.org/content/363/6433/1287.full (dostęp: 4.05.2020 r.).

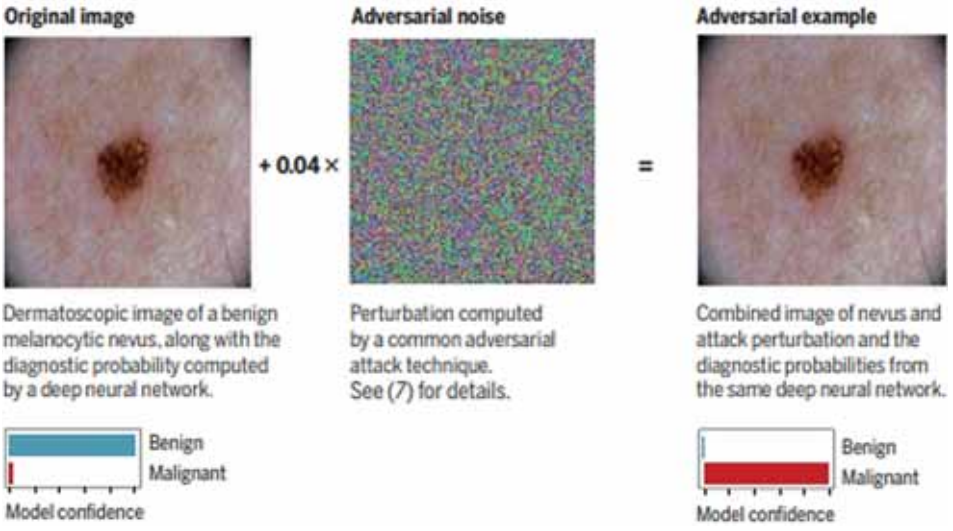


Systemy głębokiego uczenia się (ang. *deep learning*) stały się popularne w przypadku medycznych analiz obrazu, takich jak diagnoza raka. Jednak ostatnie badania pokazują, że medyczne systemy głębokiego uczenia się mogą zostać oszukane przez starannie zaprojektowane ataki z niewielkimi niedostrzegalnymi zaburzeniami. Powoduje to obawy dotyczące bezpieczeństwa związanego z wdrażaniem tych systemów w warunkach klinicznych.

Na rysunku 2.16 przedstawiono modyfikację znamienia na skórze o łagodnym przebiegu w celu jego identyfikacji jako zmiany rakowej.

Rysunek 2.16. Zmiana wyniku klasyfikacji przez dodanie szumu opracowanego antagonistycznym systemem uczącym się

Źródło: Finlayson, S.G. i in. (2019). *Adversarial attacks on medical machine learning*. https://science.sciencemag.org/content/363/6433/1287.full (dostęp: 4.05.2020 r.).



Automatyczna diagnostyka może wskazać retinopatię cukrzycową, choroby płuc czy raka skóry przy rzeczywistym braku tych chorób, co istotnie wskazuje na podatność medycznych modeli opartych na głębokim uczeniu się na zakłócenia (rys. 2.17).

Rysunek 2.17. Zakłócenia wprowadzane do obrazów medycznych

Źródło: Ma, X. i in. (2020). *Understanding Adversarial Attacks on Deep Learning Based Medical Image Analysis Systems*, https://arXiv.org/pdf/1907.10456.pdf (dostęp: 4.05.2020 r.).