

## Maryland and New Jersey Update Their Data Breach Laws

September 26, 2019 – Both Maryland and New Jersey have made recent changes to their data breach laws. The changes will significantly increase consumer protections in these states.

Tweet

```
(function() {
var s = document.createElement('SCRIPT'), s1 = document.getElementsByTagName('SCRIPT')[0];
s.type = 'text/javascript';
s.src = 'http://widgets.digg.com/buttons.js';
s1.parentNode.insertBefore(s, s1);
})();
```

```
(function() {
var po = document.createElement('script'); po.type = 'text/javascript'; po.async = true;
po.src = 'https://apis.google.com/js/plusone.js';
var s = document.getElementsByTagName('script')[0]; s.parentNode.insertBefore(po, s);
})();
```

The updates to New Jersey's law essentially update the state's definition of "personally identifiable information" to include an email address or a user name when combined with a password or the answers to security questions. The change makes it the 11th state to include information that can lead to online account take-overs by hackers. It went into effect on September 1st.

An equally significant update to Maryland's data breach notification law will go into effect on October 1st. From that point on, health providers will be required to notify the state's Insurance Administration when patient data is exposed in a breach.

The change in Maryland's law impacts HMOs, insurance companies, healthcare providers and insurance administrators. Notification to the state is required when a person's name is included in a breach along with unencrypted standard PII, an insurance policy number or a medical record number. Furthermore, if the party breached believes that breached data may be misused, notification is required even in cases where the data is encrypted.

by Jim Malmberg

Note: When posting a comment, please sign-in first if you want a response. If you are not registered, [click here](#). Registration is easy and free.

Follow ACCESS